Knowledge security in a polarized world

Arthur Mol

Wageningen University & Research

University = openness

- University: open & free exchange of
  - information,
  - results
  - Staff & students
- Recently Open Science:
  - Open access
  - Open/FAIR data
  - Open education

UNIVERSITY

CORPORATE
ESPIONAGE

Growing political attention

- Growing political attention to the risks of unwanted knowledge transfer
    - Threat (hybrid) warfare
    - Loss of national competitive position/innovation strength
    - Growing geopolitical dominance in basic goods and services (energy, telecom, food, medicines, etc)
    - Pressure on staff/students; (self) censorship
- Stronger regulation of export of knowledge
- Requests to knowledge institutions to mitigate and control the risks of unwanted knowledge transfer
- Growing interest of national secret services
- With populist politics: polarization debate on universities

Knowledge security and cyber security

- Cyber security: measures to protect computers, networks, programs and data from unauthorized access or attacks
- One of the *measures* to mitigate and control knowledge security risks
- Other measures:
  - Physical security, e.g controlled access to laboratories
  - HR policy, e.g screening (future) employees/students
  - Due diligence on potential collaborations

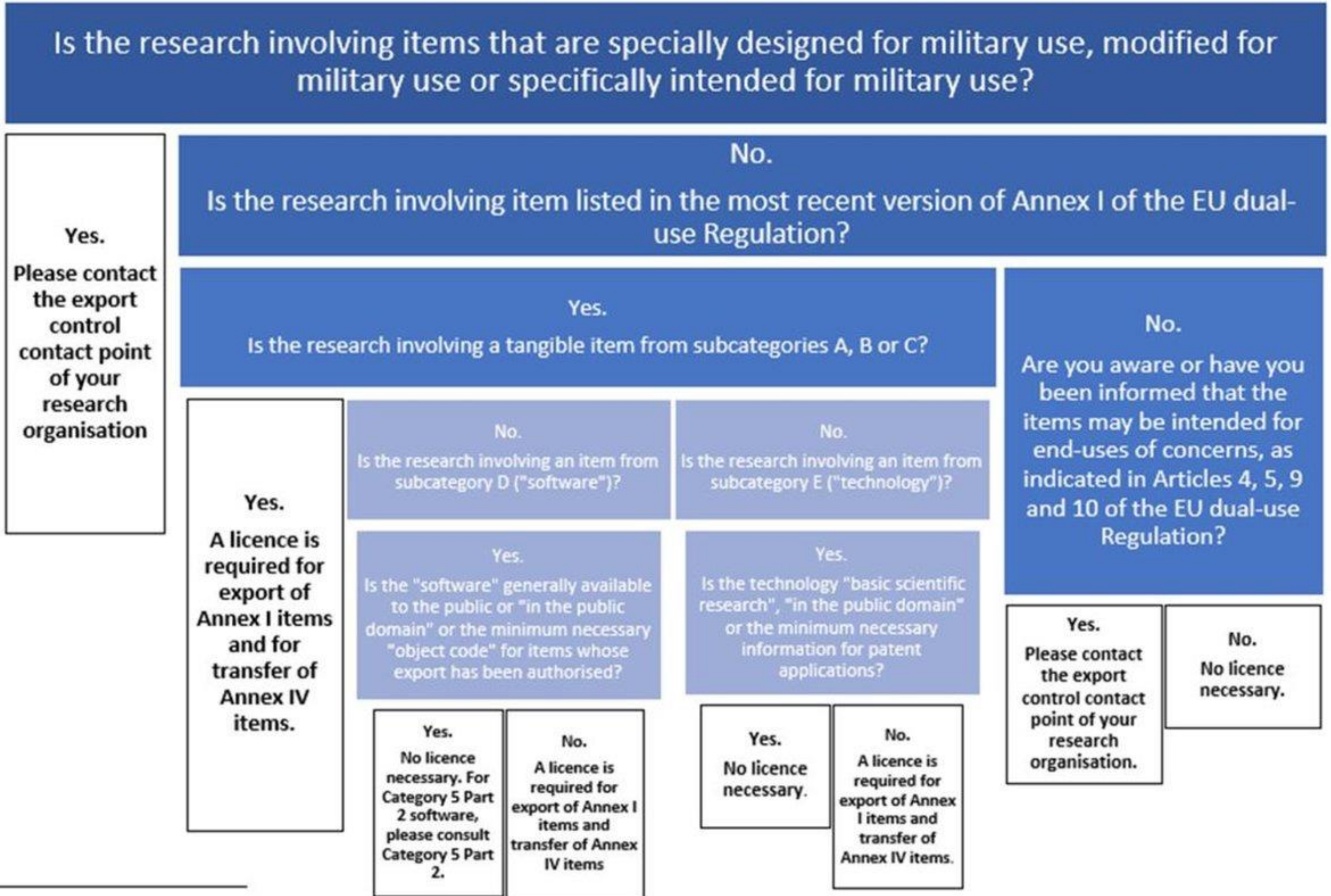
What is new?

- Military security: not new
- Economic security: not new
- Multi-polar and polarized world: relatively new
- Cyber security: relatively new
- Task/responsibility for university: relatively new

EU regulates export of sensitive knowledge

- all military goods, items, technology and knowledge thereof;
- all dual-use goods, items, technology and knowledge thereof (Dual Use Regulation 2021/821).

EU toolkit for mitigating ‘foreign interference’



Is the research involving items that are specially designed for military use, modified for military use or specifically intended for military use?

Yes.
Please contact the export control contact point of your research organisation

No.
Is the research involving item listed in the most recent version of Annex I of the EU dual-use Regulation?

Yes.
Is the research involving a tangible item from subcategories A, B or C?

Yes.
A licence is required for export of Annex I items and for transfer of Annex IV items.

No.
Is the research involving an item from subcategory D ("software")?

Yes.
Is the "software" generally available to the public or "in the public domain" or the minimum necessary "object code" for items whose export has been authorised?

Yes.
No licence necessary. For Category 5 Part 2 software, please consult Category 5 Part 2.

No.
A licence is required for export of Annex I items and transfer of Annex IV items

No.
Is the research involving an item from subcategory E ("technology")?

Yes.
Is the technology "basic scientific research", "in the public domain" or the minimum necessary information for patent applications?

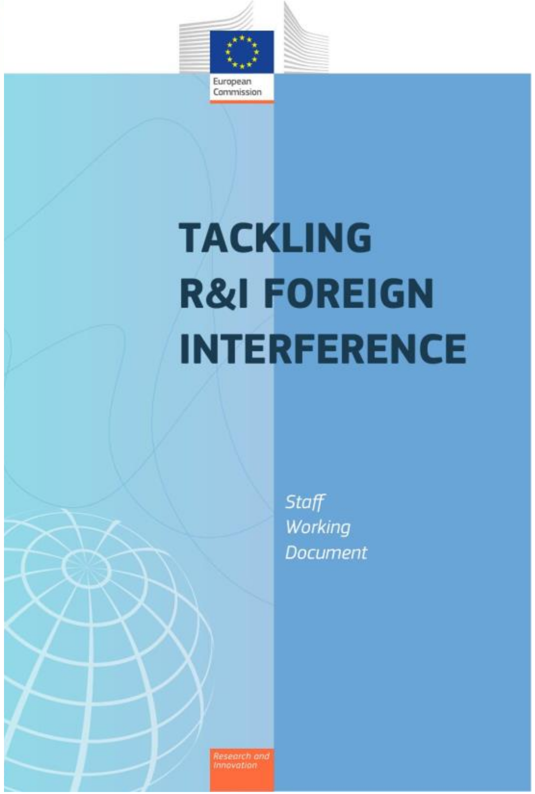
Yes.
No licence necessary.

No.
A licence is required for export of Annex I items and transfer of Annex IV items.

No.
Are you aware or have you been informed that the items may be intended for end-uses of concerns, as indicated in Articles 4, 5, 9 and 10 of the EU dual-use Regulation?

Yes.
Please contact the export control contact point of your research organisation.

No.
No licence necessary.



European Commission

TACKLING R&I FOREIGN INTERFERENCE

Staff Working Document

National guidelines

- Australia (2019): Guidelines to counter foreign interference in the Australian university sector
- Sweden (2020): Responsible internationalisation: Guidelines for reflection on international academic collaboration
- UK (2020): Managing Risks in Internationalisation: security related issues
- Germany (2020): Leitlinien und Standards für international Hochschulkooperationen
- The Netherlands (2021): Framework Knowledge Security Dutch Universities
- Canada (2021): Safeguarding your research
- Etc.......

Consequences for universities

- Management attention
- Spending € resources on security
- Assessing and changing collaboration, partners, etc.
- Internal debates and confusion
- New (media/reputation) vulnerabilities
- New lines of control: secret services, public watchdogs

Dilemmas and questions for universities

- ‘Sensitive technologies’ and dual use: many grey areas
    - e.g gmo technology, GIS, AI, sensing technologies

- Tension between academic freedom/open science and knowledge security
    - Confusion among staff

- Tension between academic freedom/autonomy and ‘contributing to the national innovation strength’
    - Is protecting national innovation strength a goal of an individual knowledge institution?

- Employees/students from *'specific countries that require attention’*.
    - discrimination or profiling based solely on nationality or ethnicity versus core values of inclusiveness

Thank you

WAGENINGEN
UNIVERSITY & RESEARCH

The Wageningen approach

- Knowledge security embedded in (international) collaboration with *individuals, organisations, regimes and countries.*
- Related to physical safety, (scientific) integrity, academic freedom, human rights, political/social/cultural values
- *Integral* assessment (including knowledge security risks) of individual collaborations responsibility of the line organization
- No screening based solely on nationality or ethnicity
- Knowledge Security Advisory Team as part of International Cooperation Advisory Team